UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/492,273	01/27/2000	Wolfgang Rankl	JEK/Rankl	9676

7590 02/11/2004

J. Ernest Kenney
Bacon & Thomas PLLC
625 Slaters Lane
4th Floor
Alexandria, VA 22314-1176

EXAMINER	
SIMITOSKI, MICHAEL J	
ART UNIT	**PAPER NUMBER**
2134	8

DATE MAILED: 02/11/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/492,273	Applicant(s) RANKL, WOLFGANG	
	Examiner Michael J Simitoski	Art Unit 2134	

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 December 2003*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-9* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-9* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *27 January 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

NORMAN M. WRIGHT
PRIMARY EXAMINER

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Applicants claim for foreign priority is acknowledged, as all necessary conditions have been met.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1 & 3-8 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent 4,200,770 to Hellman et al. (Hellman) in view of U.S. Patent 6,038,551 to Barlow et al. (Barlow).

Regarding claims 1 & 3, Hellman discloses a system wherein two conversers communicate over an insecure channel in substantially the same method as described in the claim (see col. 3, lines 41-68, col. 4, lines 1-67 and col. 5, lines 1-3). This is commonly referred to in the art as the Diffie-Hellman key-exchange algorithm. Hellman's system discloses enabling "conversers" to communicate securely even if an unauthorized party intercepts all communication between them (see col. 2, lines 5-13), but lacks application of the algorithm to a chip card and a processing station. Barlow teaches that problems that exist with card-like mechanisms, such as lack of scalability, the difficulty in having to configure millions of devices with unique keys and the replacement of keys after the manufacture of the device, can be

overcome by using customizable cards that are not bound to specific encryption keys (see col. 2, lines 17-66). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to apply Hellman's key-exchange algorithm to a smartcard system. One of ordinary skill in the art would have been motivated to perform such a modification to eliminate the need to preprogram the hardware of the smartcard with specific keys, as taught by Barlow (see col. 2, lines 17-66).

Regarding claims 4-5, Hellman discloses using modular exponentiation to determine the values to be sent from each converse and to determine the secret key (see col. 4, lines 18-67).

Regarding claim 6, Hellman discloses that the key sources may be random number generators (see col. 4, lines 1-5).

Regarding claim 7, Hellman discloses that the secure key generators generate keys that may be used in cryptographic devices (see col. 5, lines 1-3), used for enciphering and deciphering information.

Regarding claim 8, Hellman's system, as modified above, lacks transmission of additional keys to the card. Barlow teaches that to support multiple applications, the card must enable a user to transport keys from one application to another (see col. 4, lines 34-49). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to further modify Hellman's system to allow multiple keys to be transported through the medium secured by the algorithm (as taught by Hellman). One of ordinary skill in the art would have been motivated to perform such a modification to support multiple applications, as taught by Barlow (see col. 4, lines 34-49).

4. Claim 9 is rejected under 35 U.S.C. 103(a) as being unpatentable over Hellman in view of Barlow as applied to claim 8 above, and further in view of U.S. Patent 5,224,163 to Gasser et al. (Gasser). Hellman's system, as modified above, lacks removal of the original session key after the receipt of personalization information. Gasser teaches that removing a key after it's use in an authorization system ensures security even if one of the participants is compromised thereafter (see col. 15, lines 51-65). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to remove the session key from Hellman's system, as modified above, after the initial transaction was complete. One of ordinary skill in the art would have been motivated to perform such a modification to prevent compromise of both the card and the apparatus if either was compromised, as taught by Gasser (see col. 15, lines 51-65).

Response to Arguments

5. Applicant's arguments filed 13/30/2003 have been fully considered but they are not persuasive.

6. Applicant's arguments with respect to claim 2 have been considered but are moot in view of the new ground(s) of rejection.

Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over Hellman in view of Barlow as applied to claim 1 above, and further in view of "Cryptographic Identification Methods for Smart Cards in the Process of Standardization" by Hans-Peter Königs in further view of Handbook of Applied Cryptography by Menezes. Hellman discloses a system, as modified above, but lacks using an individual identifier to generate the initial value for the card.

Königs teaches that one can greatly simplify the problem of key management and make an explicit public key unnecessary by deducing a verification key from an identification word/individual identifier (see page 46). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to further modify Hellman's system to use identification information as the basis for a key. One of ordinary skill in the art would have been motivated to perform such a modification to simplify key management, as taught by Königs (see page 46). Hellman, as modified above, lacks the identification information being a serial number. However, Menezes teaches that sequence numbers can be used to identify entities, often in key establishment protocols (see §10.3.1 & §10.12). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use the serial number of the smart card for identification, and hence as the basis for the key. One of ordinary skill in the art would have been motivated to perform such a modification to provide uniqueness, as taught by Menezes (see §10.3.1 & §10.12).

7. In response to applicant's suggestion of the deficiencies of Hellman and Barlow (see page 6, §3 of the amendment/response), applicant is directed to the following:

a. Hellman, col. 4, lines 53-67, where both conversers/secret key generators (chip card and processing station) generate parts of first and second values Y_1 and Y_2 are parts of first and second "values" (a, q).

b. Hellman, col. 4, lines 44-67, where secret key generator 22 generates a secret initial value (K) from at least part of the first value (X_1) and the transmitted part of the second value (Y_2).

c. Hellman, col. 4, lines 44-67, where secret key generator 21 generates a secret initial value (K) from at least part of the second value (X_2) and the transmitted part of the first value (Y_1).

8. In response to applicant's arguments, the recitation that the Konigs, Hellman and Barlow references fail to disclose *chipcard initialization* (see page 7 of applicant's response) has not been given patentable weight because the recitation occurs in the preamble. A preamble is generally not accorded any patentable weight where it merely recites the purpose of a process or the intended use of a structure, and where the body of the claim does not depend on the preamble for completeness but, instead, the process steps or structural limitations are able to stand alone. See *In re Hirao*, 535 F.2d 67, 190 USPQ 15 (CCPA 1976) and *Kropa v. Robie*, 187 F.2d 150, 152, 88 USPQ 478, 481 (CCPA 1951).

9. In response to applicant's suggestion that the cited references fail to disclose transferring "parts" of secret initial value (pages 6-8 of applicant's response), applicant is directed to Hellman '770 col. 3, lines 40-68 & col. 4, lines 1-56. For a simplified explanation of the same protocol, applicant is directed to the previously cited Schneier reference (pages 513-514). Schneier discloses the four simplified steps of the Diffie-Hellman key exchange protocol, where Alice and Bob each have an initial value x and y, respectively. Using the values g, n, Bob calculates $Y(= g^x \bmod n)$ and Alice calculates $X(= g^y \bmod n)$. Bob transmits Y, g, n to Alice and keeps x secret, in a manner apparently identical to page 5 of the instant application's specifications, where Y, g, n represent the transmitted "part". Note also that Schneier's [496]

citation on page 513 corresponds to "New Directions in Cryptography" by Diffie et al., the basis for the Hellman '770 reference

10. In response to applicant's suggestion that Hellman discloses each converser already possessing a secret signal (page 6 of applicant's response), applicant is directed to col. 4, lines 1-10. Hellman discloses that the signals can be generated with key sources, deriving the signals from random integers.

Conclusion

11. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (703)305-8191.

The examiner can normally be reached on Monday - Thursday, 8:00 a.m. - 5:30 p.m.. The examiner can also be reached on alternate Fridays from 8:00 a.m. – 4:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (703)308-4789.

Any response to this action should be mailed to:
Commissioner of Patents and Trademarks
Washington, DC 20231
Or faxed to:
(703)746-7239 (for formal communications intended for entry)
Or:
(703)746-7240 (for informal or draft communications, please label "PROPOSED" or "DRAFT")
Hand-delivered responses should be brought to Crystal Park II, 2121 Crystal Drive, Arlington, VA 22202, Fourth Floor (Receptionist).

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-9000.

13. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MJS
February 3, 2004

NORMAN M. WRIGHT
PRIMARY EXAMINER